Red Hat Directory Server Red Hat Directory Server 9
9.0 Release Notes

for 9.0
Edition 9.0

Ella Deon Lackey

Red Hat Directory Server Red Hat Directory Server 9 9.0 Release Notes

for 9.0
Edition 9.0

Ella Deon Lackey
dlackey@redhat.com

Legal Notice

Copyright © 2011 Red Hat, Inc..

This document is licensed by Red Hat under the Creative Commons Attribution-ShareAlike 3.0 Unported License. If you distribute this document, or a modified version of it, you must provide attribution to Red Hat, Inc. and provide a link to the original. If the document is modified, all Red Hat trademarks must be removed.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, MetaMatrix, Fedora, the Infinity Logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack Logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

Release notes for Directory Server 9.0

Table of Contents

1. New in Red Hat Directory Server 9.0 . . . . . **2**
1.1. New: Renaming Subtrees and Moving to a New Parent 2
1.2. New: Introducing the Managed Entries Plug-in to Create Pairs of Entries 2
1.3. New: Introducing the Account Policy Plug-in to Define Time-Based Account Inactivation 2
1.4. Enhanced: 20-Way Multi-Master Replication 3
1.5. Enhancement: Separate Resource Limits for Simple Paged Results 3
1.6. New: Attributes for Samba Interoperability with the Retro Changelog 3
1.7. Enhanced: Added Global Entry USN Count 3
1.8. Enhanced: DNA Plug-in Handles Multiple Attributes in Same Range 3
1.9. Enhanced: Added Option to Have Separate Fractional Replication List for Total Updates 3
1.10. Enhanced: New Options and Procedures to Set up Secure Connections 4
1.11. New: Added Support for the CoS merge-schemes Qualifier 4
1.12. New: Added SELinux Policies 4
1.13. New: Replication Session Hooks 4

2. Structural Changes in Red Hat Directory Server 9.0 . . . . . **4**
2.1. Replacing MozLDAP Libraries with OpenLDAP Libraries 5
2.2. Moving the Changelog Database into the Main Database Environment 5
2.3. Allowing ID Scan List Limit to Be Set Dynamically 5
2.4. Allowing cn=config Attributes to Be Deleted 5

3. System Requirements **5**
3.1. Required JDK 5
3.2. Perl Prerequisites 6
3.3. Fonts 6
3.4. Software Conflicts 6
3.5. Directory Server Supported Platforms 6
3.6. Directory Server Console Supported Platforms 6
3.7. Windows Sync Service Platforms 6
3.8. Web Application Browser Support 7

4. Installing Directory Server 9.0 . . . . . **7**
4.1. Installing the JDK 7
4.2. Obtaining Packages 7
4.3. Running setup-ds-admin.pl 9
4.4. Upgrading to Directory Server 9.0 9

5. Basic Information about Red Hat Directory Server **11**

6. Bugs Fixed in 9.0 . . . . . **13**

7. Known Issues **16**

These release notes contain important information available at the release of Red Hat Directory Server version 9.0. New features, system requirements, installation notes, known problems, resources, and other current issues are addressed here. Read this document before beginning to use Directory Server 9.0.

1. New in Red Hat Directory Server 9.0

Directory Server 9.0 has introduced many features to make managing the directory service and its data easier.

1.1. New: Renaming Subtrees and Moving to a New Parent

Every distinguished name is comprised of a series of name elements that indicate the place of the entry within the directory tree. The far left element, the *relative* DN or RDN, is the entry's own name. The other elements identify the ancestors of the entry.

In previous releases of Directory Server, it was possible to rename leaf or terminal entries; that is, entries without children. This is a *modrdn* operation. However, it was not possible to rename a parent entry, which would subsequently end up "moving" all its children in the directory tree. Directory Server 9.0 introduces *subtree rename operations*. This allows parent entries to be renamed through a modrdn operation, and all their children are subsequently updated to maintain the directory structure. Subtree renames can also be disabled to prevent changing the directory tree.

Additionally, Directory Server now supports moving a leaf entry to a new parent, a moddn operation with a new superior.

With the combination of subtree rename and moddn with a new superior, Directory Server provides full support of the modify DN operations specified in RFC 4511.

For more information on subtree rename operations, see the 9.0 Administrator's Guide.

1.2. New: Introducing the Managed Entries Plug-in to Create Pairs of Entries

There are situations when one entry is created and there should automatically be a corresponding second entry with related attribute values. For example, when a Posix user is created, a corresponding Posix group entry should also be created.

The Managed Entries Plug-in identifies an origin entry target. When an entry is created in that scope, matching the given attributes, it automatically generates a new, managed entry.

For more information on the Managed Entries Plug-in, see the 9.0 Administrator's Guide.

1.3. New: Introducing the Account Policy Plug-in to Define Time-Based Account Inactivation

Account policies can already be set based on failed password attempts or by an administrator manually. The new Account Policy Plug-in in Directory Server 9.0 allows administrators to set time-based account lockout policies.

The Account Policy Plug-in can configure natural timeout periods for accounts based on activity (assessed by the last login time) or by the account age (based on the account creation time).

For more information on the Account Policy Plug-in, see the 9.0 Administrator's Guide.

1.4. Enhanced: 20-Way Multi-Master Replication

In previous versions of Red Hat Directory Server, multi-master replication was supported with up to four masters in a single replication topology. In 9.0, it is possible to have up to 20 masters in a replication topology.

1.5. Enhancement: Separate Resource Limits for Simple Paged Results

Resource limits set limits on searches, based on things like the number of results returned, the time of searches, and the number of entries checked. Resource limits can be applied to a user or to the entire directory.

Beginning in Directory Server 8.2, Directory Server supports *simple paged searches*, which returns paged results (chunks of the search results at a time, rather than altogether). Because the performance is better with paged searches, Directory Server 9.0 introduces new attributes to set different resource limits for paged searches and standard searches. This allows administrators to set higher resource limits for paged searches (improving user experience) while keeping the lower resource limits for regular searches (maintaining performance).

For more information on resource limits and paged searches, see the 9.0 Administrator's Guide.

1.6. New: Attributes for Samba Interoperability with the Retro Changelog

Two new attributes, ***isreplicate*** and ***nsslapd-attribute***, have been added to the Retro Changelog Plug-in to better integrate Directory Server with other applications, like Samba. The ***nsslapd-attribute*** attribute explicitly includes Directory Server attributes in the retro changelog entries; this enables operational attributes (normally excluded from replication) to be included in changelog entries and available to other servers.

1.7. Enhanced: Added Global Entry USN Count

Beginning in Directory Server 8.2, changes to entries were tracked on the local database using a local *update sequence number*. Whenever a change was made anywhere in the database, the counter was incremented up and the ***entryusn*** attribute on the entry was updated.

In Directory Server 9.0, USNs can be maintained not only on the local database, but across all databases in the directory if the USN Plug-in is set to global mode.

1.8. Enhanced: DNA Plug-in Handles Multiple Attributes in Same Range

The Distributed Numeric Assignment (DNA) Plug-in assigns unique numbers, from within a given range, automatically to given entries. In 8.2, the DNA Plug-in assigned those numbers to a single attribute type; starting in 9.0, the DNA Plug-in can assign numbers from the same range to multiple attribute types.

This allows the same number to be assigned to different attributes. For example, the DNA Plug-in can assign the same value to the ***uidNumber*** and ***gidNumber*** attributes

1.9. Enhanced: Added Option to Have Separate Fractional Replication List for Total Updates

Fractional replication allows specific attributes to be *excluded* from replication updates.

Directory Server 9.0 introduces a new attribute, ***nsDS5ReplicatedAttributeListTotal***, which sets a second list of attributes to exclude from replication, specifically from a total update. This allows different attributes to be excluded from a regular, incremental update than a total update. Very large attributes — like certificates or binary attributes — can be excluded from a regular update, but included in total

updates when data consistency is more important than performance.

TIP

Using different fractional replication lists for incremental and total updates is strongly recommended if you use the ***memberof*** plug-in. memberOf fixup tasks are run after every replication update, and this causes negatively affects server performance.
Limiting the ***memberof*** attribute to being replicated only for total updates improves the performance of replica initialization and replication.

For more information on incremental updates, total updates, and fractional replication, see the 9.0 Administrator's Guide.

1.10. Enhanced: New Options and Procedures to Set up Secure Connections

Directory Server allows secure connections to be set between servers and between servers and clients using SSL, TLS, Start TLS, or SASL. Directory Server 9.0 introduces some new options to refine what kinds of secure connections are allowed and to administer secure connections more easily:

- Procedures have been added to allow administrators how to disable selected SASL mechanisms.
- Procedures have been added to disable SSLv3 and require TLS connections only.
- A new attribute has been added to allow the Directory Server to be restarted with an expired certificate. This means that the server can still run and operate until the expired certificate is replaced.

1.11. New: Added Support for the CoS merge-schemes Qualifier

A class of service adds and updates an attribute in an entry based on changes in an identified template entry. Normally, when a change is made to the CoS attribute, the new value overwrites any previous attribute in the entry. The new *merge-schemes* qualifier for CoS definitions tells the CoS to add attributes and allow multiple values, rather than replacing attributes when the CoS changes.

1.12. New: Added SELinux Policies

SELinux is a security function in Linux that categorizes files, directories, ports, processes, users, and other objects on the server. New policies have been written for Directory Server files, directories, and ports. In 9.0, Directory Server can run with SELinux set to enforcing mode and operate normally.

The 9.0 Administrator's Guide has information on the default Directory Server policies and simple procedures for changing and updating these policies. More detail about SELinux and Red Hat Enterprise Linux is covered in the SELinux Guide.

1.13. New: Replication Session Hooks

Client applications can have some control over replication operations by using custom plug-ins that define *replication session hooks*. Suppliers and consumers can send each other some limited information. If both servers meet the required session settings in the plug-in (like using the same Directory Server version), then replication proceeds; if not, it fails.

The new replication callbacks are detailed in the Plug-in Programmer's Guide.

2. Structural Changes in Red Hat Directory Server 9.0

Along with its new features, Directory Server 9.0 has introduced some structural changes to the way that its tools and databases which are worthwhile to note.

2.1. Replacing MozLDAP Libraries with OpenLDAP Libraries

The Mozilla LDAP client libraries have been replaced with OpenLDAP client libraries. The most visible effect of this change is that all of the LDAP tools have been replaced with OpenLDAP tools.

One aspect of this change is that OpenLDAP command-line tools, such as **`ldapsearch`**, use SASL connections by default. To disable SASL and use a simple bind or an SSL/TLS connection, use the **`-x`** option with the command-line tool.

2.2. Moving the Changelog Database into the Main Database Environment

In previous versions of Directory Server, the changelog (replication) database was kept in a separate environment than the main database. This negatively impacted overall performance in two ways:

- It increased the amount of storage and memory required for the Directory Server.
- The changelog database was not included in Directory Server backups, which meant that every restore operation required every consumer to be re-initialized.

By moving the changelog database into the main database environment, the overall Directory Server performance is improved.

2.3. Allowing ID Scan List Limit to Be Set Dynamically

The ID list scan limit is a resource limit that restricts how many entries are loaded from an index in a search before the search is treated as an unindexed search. Previously, changing this attribute required a server restart. In 9.0, this value can now be set dynamically.

2.4. Allowing cn=config Attributes to Be Deleted

Core configuration attributes cannot be deleted, by default. Even if values are not present in the **`dse.ldif`** file, the Directory Server uses default values for core attributes. A new configuration attribute, ***`nsslapd-allowed-to-delete-attrs`***, sets a list of core configuration attributes which can be deleted.

3. System Requirements

This section contains information related to installing and upgrading Red Hat Directory Server 9.0, including prerequisites and hardware or platform requirements.

3.1. Required JDK

Red Hat Directory Server 9.0 requires Sun JRE 1.6.0 or OpenJDK 1.6.0 for Red Hat Enterprise Linux 6.

IMPORTANT

When the new JDK is installed for Directory Server 9.0, it is no longer possible to manage older instances of Directory Server using the Directory Server Console because the required JDKs for the different Directory Server versions are different. You must migrate any older instance to Directory Server 9.0 if you need to manage that instance with the Directory Server Console.

3.2. Perl Prerequisites

Directory Server 9.0 does not package **nsperl** with the product. **perldap** should work with the version of **perl** pre-installed on the system.

Use the Perl version that is installed with the Red Hat Enterprise Linux operating system in **/usr/bin/perl** for both 32-bit and 64-bit versions of Red Hat Directory Server.

3.3. Fonts

A font package must be installed before the Directory Server Console can be launched. Any font package is acceptable.

3.4. Software Conflicts

Directory Server cannot be installed on any system that has a Red Hat Enterprise Linux Identity Management server installed. (The Identity Management server is also called an *IPA server*.)

Likewise, no Red Hat Enterprise Linux Identity Management server can be installed on a system with a Directory Server instance.

3.5. Directory Server Supported Platforms

Directory Server 9.0 is supported on the following platforms:

- Red Hat Enterprise Linux 6 x86 (32-bit)
- Red Hat Enterprise Linux 6 x86_64 (64-bit)

NOTE

Red Hat Directory Server 9.0 is supported running on a virtual guest on a Red Hat Enterprise Linux virtual server.

3.6. Directory Server Console Supported Platforms

The Directory Server Console is supported on the following platforms:

- Red Hat Enterprise Linux 6 i386 (32-bit)
- Red Hat Enterprise Linux 6 x86_64 (64-bit)
- Microsoft Windows Server 2008 (32-bit)
- Microsoft Windows Server 2008 (64-bit)

NOTE

The Directory Server Console can be installed on additional Windows platforms at an additional cost.

3.7. Windows Sync Service Platforms

The Windows Sync tool runs on these Windows platforms:

- Active Directory on Microsoft Windows Server 2008 (32-bit)

- Active Directory on Microsoft Windows Server 2008 (64-bit)

3.8. Web Application Browser Support

Directory Server 9.0 supports the following browsers to access web-based interfaces, such as **Admin Express** and online help tools:

- Firefox 3.x
- Microsoft Internet Explorer 6.0 and higher

4. Installing Directory Server 9.0

For more detailed instructions on installing Directory Server 9.0, see the *Directory Server Installation Guide*.

4.1. Installing the JDK

Directory Server 9.0 requires either Sun JRE 1.6.0 or OpenJDK 1.6.0.

For example:

```
yum install java-1.6.0-openjdk
```

OpenJDK is also available for download from http://openjdk.java.net/install/.

IMPORTANT

When the new JDK is installed for Directory Server 9.0, it is no longer possible to manage older instances of Directory Server using the Directory Server Console because the required JDKs for the different Directory Server versions are different. You must migrate any older instance to Directory Server 9.0 if you need to manage that instance with the Directory Server Console.

4.2. Obtaining Packages

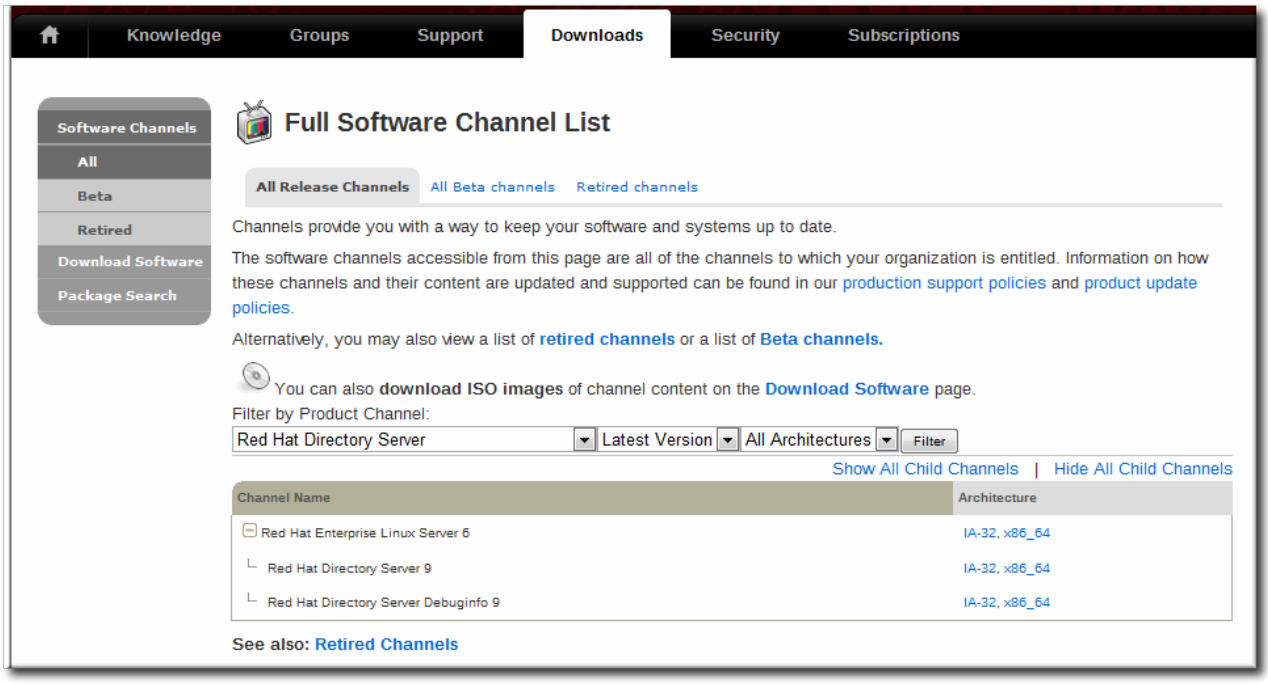
The simplest way to install Red Hat Directory Server 9.0 is using the **yum** command:

```
yum install redhat-ds* redhat-idm-console
```

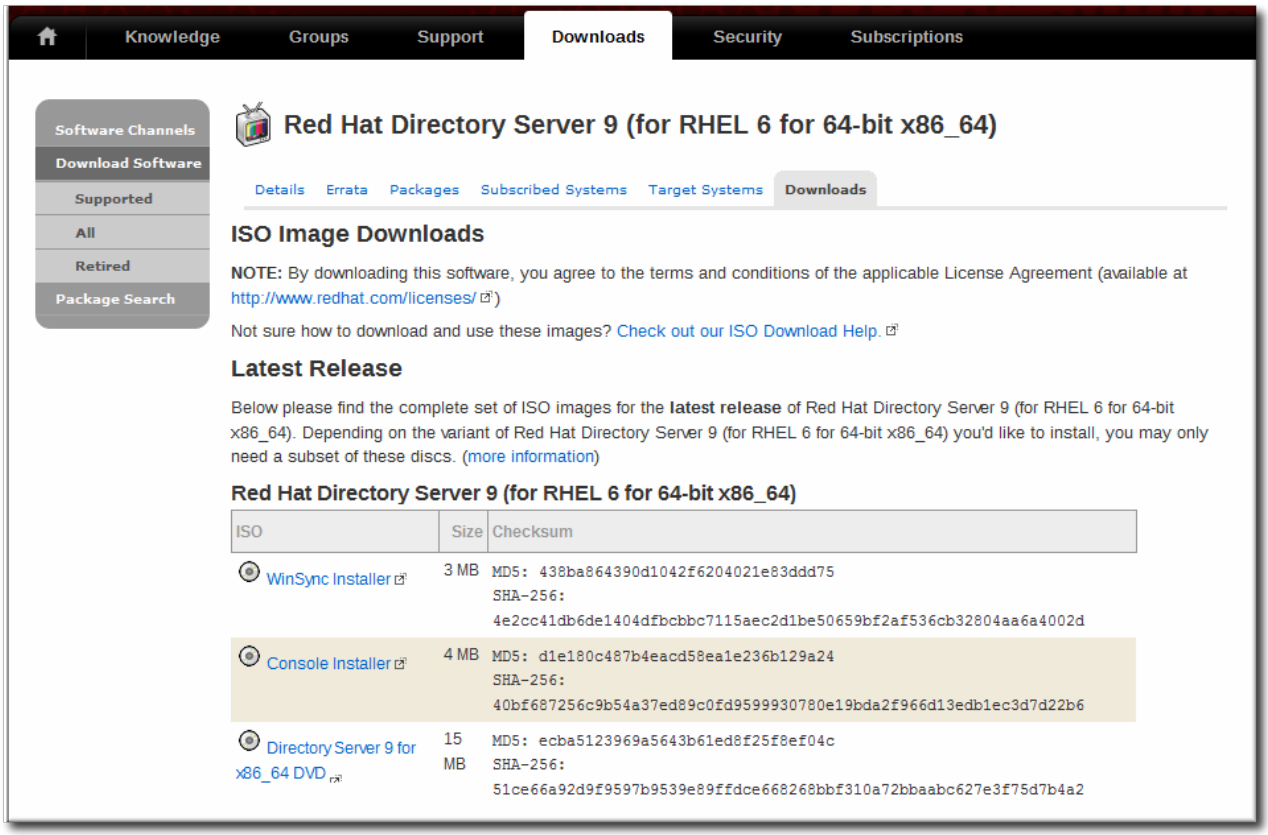
RPM packages can be downloaded from Red Hat Network:

1. Go to http://access.redhat.com.

   Downloading packages from Red Hat Network requires specific entitlements for the account for the 9.0 release.
2. Click the **Downloads** tab, and select the Red Hat Enterprise Linux channels.


Knowledge
Groups
Support
Downloads
Security
Subscriptions
Software Channels
All
Beta
Retired
Download Software
Package Search
Full Software Channel List
All Release Channels
All Beta channels
Retired channels
Channels provide you with a way to keep your software and systems up to date.
The software channels accessible from this page are all of the channels to which your organization is entitled. Information on how these channels and their content are updated and supported can be found in our production support policies and product update policies.
Alternatively, you may also view a list of retired channels or a list of Beta channels.
You can also download ISO images of channel content on the Download Software page.
Filter by Product Channel:
Red Hat Directory Server
Latest Version
All Architectures
Filter
Show All Child Channels | Hide All Child Channels
Channel Name
Architecture
Red Hat Enterprise Linux Server 6
IA-32, x86_64
Red Hat Directory Server 9
IA-32, x86_64
Red Hat Directory Server Debuginfo 9
IA-32, x86_64
See also: Retired Channels

3. Set the product to filter for **`Red Hat Directory Server`**.
4. Select the architecture.
5. Open the **`Downloads`** tab, and begin downloading the ISO.


Knowledge
Groups
Support
Downloads
Security
Subscriptions
Software Channels
Download Software
Supported
All
Retired
Package Search
Red Hat Directory Server 9 (for RHEL 6 for 64-bit x86_64)
Details
Errata
Packages
Subscribed Systems
Target Systems
Downloads
ISO Image Downloads
NOTE: By downloading this software, you agree to the terms and conditions of the applicable License Agreement (available at http://www.redhat.com/licenses/)
Not sure how to download and use these images? Check out our ISO Download Help.
Latest Release
Below please find the complete set of ISO images for the latest release of Red Hat Directory Server 9 (for RHEL 6 for 64-bit x86_64). Depending on the variant of Red Hat Directory Server 9 (for RHEL 6 for 64-bit x86_64) you'd like to install, you may only need a subset of these discs. (more information)
Red Hat Directory Server 9 (for RHEL 6 for 64-bit x86_64)
ISO
Size
Checksum
WinSync Installer
3 MB
MD5: 438ba864390d1042f6204021e83ddd75
SHA-256:
4e2cc41db6de1404dfbcbbc7115aec2d1be50659bf2af536cb32804aa6a4002d
Console Installer
4 MB
MD5: d1e180c487b4eacd58ea1e236b129a24
SHA-256:
40bf687256c9b54a37ed89c0fd9599930780e19bda2f966d13edb1ec3d7d22b6
Directory Server 9 for x86_64 DVD
15 MB
MD5: ecba5123969a5643b61ed8f25f8ef04c
SHA-256:
51ce66a92d9f9597b9539e89ffdce668268bbf310a72bbaabc627e3f75d7b4a2

6. Install the packages using **`rpm`**.

```
ls *.rpm | egrep -iv -e devel -e debuginfo | xargs rpm -ivh
```

The **`PassSync.msi`** installer is available in the WinSync package in the Directory Server channel, through the **`Downloads`** tab, same as the ISO image. Download this file to the Windows machine, and then double-click the icon and go through the installer.

NOTE

There are two PassSync packages available, one for 32-bit Windows servers and one for 64-bit. Make sure to select the appropriate packages for your Windows platform.

4.3. Running setup-ds-admin.pl

After installing the packages, run the **`setup-ds-admin.pl`** script to configure the new Directory Server and Admin Server instances. For example:

```
setup-ds-admin.pl
```

See the *Directory Server Installation Guide* for more information about **`setup-ds-admin.pl`** script options and the Directory Server configuration interface.

4.4. Upgrading to Directory Server 9.0

This upgrade procedure assumes that the original machine and the new machine have the same architecture (i.e., both are 32-bit machines or both are 64-bit machines).

NOTE

Upgrade is only supported from 8.2 to 9.0. Other versions of Red Hat Directory Server should be migrated to 8.2 and then upgraded to 9.0.

WARNING

Migration *cannot* change the hostname used by the Directory Server and Admin Server.

1. Stop the Directory Server and Admin Server.

   ```
   service dirsrv-admin stop
   service dirsrv stop
   ```

2. Back up all the Directory Server user and configuration data. For example:

   ```
   cd /usr/lib/dirsrv/slapd-instance_name

   db2bak /var/lib/dirsrv/slapd-instance_name/bak/instance_name-
   2011_04_30_16_27_56
   ```

3. Tar (almost) all of the files and directories for the original Directory Server 8.2 instance.

   The **`admserv.conf`** and **`httpd.conf`** files should not be included since the new versions of these files should always be used. Additionally, these tar files don't contain the error and access log files. These files are not necessary for upgrading an instance but can be stored separately.

IMPORTANT

Make sure that partition where the tar file is created has enough space to store all of the configuration and data.

```
[root@server1 ~]# cd  /

[root@server1 ~]# tar cpjf rhds-upgrade.tar.bz2 -C / --no-recursion --exclude
httpd.conf --exclude admserv.conf etc/sysconfig/dirsrv* etc/dirsrv/slapd-*
etc/dirsrv/slapd-*/* etc/dirsrv/slapd-*/schema/* var/run/dirsrv
var/lock/dirsrv/slapd-* var/log/dirsrv/slapd-* var/lib/dirsrv/slapd-*
var/lib/dirsrv/slapd-*/* var/lib/dirsrv/slapd-*/ldif/*
var/lib/dirsrv/slapd-*/db/* var/lib/dirsrv/slapd-*/db/*/* etc/dirsrv/admin-
serv etc/dirsrv/admin-serv/* var/log/dirsrv/admin-serv var/lib/dirsrv/slapd-
*/cldb/* usr/lib[64]/dirsrv/slapd-*
```

NOTE

The **cldb** location assumes that the changelog is located in the default changelog directory. If the changelog is in a different location, use the appropriate directory. If replication is not enabled, this directory can be omitted.

4. On the new machine which will host Directory Server, install or upgrade the Directory Server 9.0 packages. For example:

```
yum install redhat-ds
```

5. Copy over the tar file to the new machine.
6. Open the root directory, and then unpack the tar file. For example:

```
cd /

tar xfjp /path/to/rhds-upgrade.tar.bz2
```

7. Make sure that the new Directory Server instance is not running.

```
service dirsrv-admin stop
service dirsrv stop
```

8. Run the **setup-ds.pl** command in offline mode to upgrade only the Directory Server configuration. This performs all of the basic setup required to perform any schema or data changes.

   For example:

```
setup-ds.pl -u -s General.UpdateMode=offline
```

9. Start the servers.

```
service dirsrv-admin start
service dirsrv start
```

10. Run the **setup-ds-admin.pl -u** script to update the configuration. Make sure that the Directory Server and Admin Server are running when the script is run.

```
setup-ds-admin.pl -u
```

11. Update syntaxes and the enable syntax checking.

    In 8.2, syntax checking is available, but disabled by default, while a new 9.0 instance has syntax checking enabled by default. Syntax validation checks every modification to attributes to make sure that the new value has the required syntax for that attribute type, so this is a beneficial configuration attribute to use to ensure data quality.

    a. Run the **syntax-validate.pl** Perl script to validate and, if necessary, correct any syntax errors in the migrated 8.2 data.

```
/usr/lib64/dirsrv/instance_name/syntax-validate.pl -D "cn=directory
manager" -w secret -b "dc=example,dc=com"
```

    b. Enable syntax checking for the migrated server.

```
/usr/lib64/mozldap/ldapmodify -D "cn=directory manager" -w secret -p
389

dn: cn=config
changetype: modify
replace: nsslapd-syntaxcheck
nsslapd-syntaxcheck: on
```

12. Verify that the directory databases have been successfully migrated. Directory Server 9.0 normalizes DN syntax during the upgrade import process. Make sure that the upgraded database is functional and contains all the data before deleting the backups.

    Search an entry which could contain escaped characters; the DNs should be updated. For example, for a DN which was previously **cn="a=abc,x=xyz"**:

```
/usr/lib64/mozldap/ldapsearch -b "dc=example,dc=com" '(cn=\"*\")' entrydn
dn: cn=a\3Dabc\2Cx\3Dxyz,dc=example,dc=com
entrydn: cn=a\3dabc\2cx\3dxyz,dc=example,dc=com
```

    If the search results are correctly escaped, the original database backend instance directory can be removed.

5. Basic Information about Red Hat Directory Server

This is some basic information for using and managing Directory Server. The Directory Server information is explained in much more detail in the *Administrator's Guide*.

Starting and Stopping the Directory Server and Admin Server

The Directory Server and Admin Server instances are started and stopped using basic service command line tools. For example, on Red Hat Enterprise Linux:

```
service dirsrv-admin start
service dirsrv start
```

Running just **service dirsrv start** starts all instances of the Directory Server on the host machine. To start a single instance, use the name of the instance in the command:

```
service dirsrv start example
```

Starting the Directory Server Console

To start the Directory Server Console, run the **redhat-idm-console** command.

```
redhat-idm-console
```

It is also possible to specify the user to log into the Console as using the **-u** and **-w** options and to give the URL to the Admin Server using the **-a** option.

```
redhat-idm-console -u "cn=Directory Manager" -w secret -a
http://ldap.example.com:9830
```

Default Port Numbers

These are the default port numbers for the Directory Server and Admin Server:

- The standard LDAP port is **389**.
- The secure (SSL) LDAPS port is **636**.
- The Admin Server port is **9830**.

Directory Server File Locations

Red Hat Directory Server 9.0 conforms to the Filesystem Hierarchy Standards. For more information on FHS, see the FHS homepage, http://www.pathname.com/fhs/. The files and directories installed with Directory Server are listed in the tables below for each supported platform.

Table 1. Basic Directory Locations

File or Directory	Location
Log files	/var/log/dirsrv/slapd-*instance*
Configuration files	/etc/dirsrv/slapd-*instance* /var/lib/dirsrv/slapd-*instance*
Instance directory	/usr/lib/dirsrv/slapd-*instance* on 32-bit systems /usr/lib64/dirsrv/slapd-*instance* on 64-bit systems
Database files	/var/lib/dirsrv/slapd-*instance*/db
Certificate and key databases	/etc/dirsrv/slapd-*instance*
Schema files	/etc/dirsrv/slapd-*instance*/schema
Runtime files	/var/lock/dirsrv/slapd-*instance* /var/run/dirsrv/
Tools	/usr/bin/ /usr/sbin/

UTF-8 and Language Support

Directory Server supports all international charactersets by default because directory data is stored in UTF-8. UTF-8 characters are fully supported for all DNs and DN components. Web services can be customized to display charactersets other than UTF-8, though UTF-8 and Latin-1 are the default for Directory Server web applications.

Directory Server can also use specified matching rules and collation orders based on language preferences in search operations.

The locales and charactersets supported by Directory Server are listed in more detail in Appendix D, "Internationalization," in the *Administrator's Guide*.

6. Bugs Fixed in 9.0

Along with new features, Directory Server 9.0 contains many bug fixes for all functional areas, features, and components in the directory service and associated tools, as well as the documentation. The complete list of bugs fixed in Directory Server 9.0 are listed in the tracking bug for this release, Bugzilla 434915. Many of the most important bugs are listed in Table 2, “List of Bugs Fixed in 9.0”.

Table 2. List of Bugs Fixed in 9.0

Bug Number	Description
151705	The Admin Server Console is hard-coded to set all TLS ciphers to enabled. Disabling the TLS ciphers through the Console is not saved, and the ciphers are re-enabled when the Admin Server is restarted.
472131 564448	Directory Server stores entry IDs in an ID list in a duplicate btree. If the ID list is very long, the internal database uses internal pages to sort the entries. When verifying database data, Berkeley DB's verify function returns *out-of-order key* errors because the database verification does not differentiate between the duplicate btree ID list and the main tree entry pages. The database, then, incorrectly tries to compare the main database page to itself rather than the duplicate ID btree. This affects Directory Server client tools such as **`verify-db.pl`** and **`dbverify`**. This issue has been fixed in BerkeleyDB 4.8.26. However, the fix will not be available for Red Hat Enterprise Linux 4 and is not yet available for Red Hat Enterprise Linux 5. It will be addressed for Red Hat Enterprise Linux 5 systems in later errata.
494944	If a ***`gidNumber`*** attribute was deleted from a replicated entry and more than one supplier was configured with the DNA Plug-in, then both masters would assign a new ***`gidNumber`*** value.
505722	An Active Directory group with a mail attribute could not be synced over to Directory Server.
522055	If an entry was moved outside the scope of the Linked Attributes Plug-in, the linked attributes were still updated.
596521	Import operations encounter fatal failures on some environments when trying to create an index for more than 200 attributes.
616850	An **`ldapmodify`** command failed to reject a replace operation for an unknown attribute.
618897	The Directory Server Console could not manage certificates if there were several instances configured on a machine with different system user IDs, even if they used the same group account.
623118	A simple paged search went into an infinite loop if the search base had a subsuffix.
668619	A high volume of TCP traffic could cause the slapd process to quit responding to clients.

694336	When synchronizing groups, Directory Server added the ***userAccountControl*** attribute to the group. However, that attribute is only allowed for users in Active Directory, which caused the sync operation to fail with an object class violation error.
694571	Editing a replication agreement to use SASL/GSS-API could fail with GSS-API errors in the error log.
695779	Adding a ***uniquemember*** attribute to a group that is synced with Active Directory would delete all the old members from the group in Active Directory, which would then backfill and delete all members from the group in Directory Server.
697694	In multi-master replication with a hub, the update operation is async, done in separate threads. The msgid corresponding to a request may not be sent to the right thread, which caused "Bad parameter to an LDAP routine" errors. This causes hard failures to eventually propagate up and halt replication with fatal errors.
706179	If an administrator created a new object class and selected the ***entryusn*** attribute as on of its allowed attributes, the Directory Server could not restart.
711679	Attempting to delete a VLV on a consumer could cause the server and the Directory Server Console to hang.
711906	The ns-slapd process segfaulted if suffix referrals were enabled.
714310	If a chained database was replicated, the server could segfault during the import operation of replication setup.
716980	If an entry was modified on RHDS and the corresponding entry was deleted on the Windows side, the sync operation attempts to pull an old version of the entry from a private file, resulting in sync using the wrong entry.
718303	Intensive update loads on master servers could break the cache on the consumer server, causing it to crash.
720059	Adding an entry with an RDN containing a percent sign (%) can caused the server to crash.
725953	Directory Server user entries with a comma in the CN failed to sync over to Active Directory.
729817	If a synced user subtree on Windows was deleted and then a user password was changed on the RHDS, the DS would crash.
735217	Doing a simple paged results search against a subtree that used IP- or DNS-based ACIs hung

	the server.
740959	Importing a CA certificate through the Directory Server Console imported the certificate into the Admin Server certificate database, not the Directory Server certificate database.

7. Known Issues

The following are some of the most important known issues in Directory Server 9.0. If applicable, supported workarounds are also described.

Table 3. Known Issues in Directory Server 9.0

Bug Number	Description	Workaround
158369	The sync attribute mapping for groups includes a number of attributes that are not actually legal on group objects, such as l, ou, and o. If someone creates an ntGroup entry with any of these attributes that is not an ou, the sync'ed entry add will fail on Active Directory because of a schema violation.	
182509	The changelog used for replication stores passwords in clear text in order to replicate them. In some contexts, this could be a security risk.	Enable fractional replication and specifically exclude the ***userPassword*** attribute from being replicated, which prevents passwords from being written to the changelog. For example: *nsds5ReplicatedAttributeListTotal: (objectclass=*) $ EXCLUDE userPassword*
190862	Global syntax checking attributes should be enforced if the settings aren't configured in the local password policy. However, if both global and local password policies are configured, the global policies aren't being enforced as the default.	1. Enable global syntax checking. 2. Enable fine-grained password checking. 3. Edit the local password policy to contain all password syntax attributes. Set the values to something other than the default settings, as listed in the *Configuration, Command, and File Reference*. 4. Re-edit the local password policy with the desired values, even if they are the defaults.
191772	If the configuration Directory Server is unavailable, Admin Express shows an internal server error. The task to access the Admin Express web page cannot be authenticated, so the attempt to open the page fails.	
510182	If the DNA Plug-in was triggered during an account creation or	

	update operation but that operation fails, the DNA counter is still incremented. This means that there is a gap in the range, where the number is used up but not assigned to an entry attribute.	
628911	If a subtree-level rename operation is performed on a subtree which contains either groups or group member entries, the ***memberof*** pointers in the user entries are not automatically updated with the new subtree name by the MemberOf Plug-in.	Run a memberof fixup task or the **fixup-memberof.pl** command to force the ***memberof*** attributes to be updated.
667943	Restarting the Directory Server hangs if a pipe file is present but the **ds-logpipe.py** script is not running.	
712202	If a replication agreement is configured with an unresolvable hostname, it returns a generic error rather than an indication that the hostname cannot be resolved: `[09/Jun/2011:14:21:21 -0400] slapi_ldap_bind - Error: could not send bind request for id [(anon)] mech [EXTERNAL]: error -1 (Can't contact LDAP server) 0 (unknown) 0 (Success)`	Change the password policy attributes from the command line.
712845	The Directory Server Console does not allow you to set password policy-related time (such as expiration time or user change time) in hours, minutes, or seconds.	Change the password policy attributes from the command line.
727659	If a ***dnaScope*** value has an unescaped space in the value, then DNA quits working after migration from Directory Server 8.1.	Remove the space from the DN in the ***dnaScope*** value.
622957 723029	There are a lot of problems associated with trying to load certificates on hardware security modules (HSMs) using the	Use NSS tools such as **certutil** to install certificates on HSMs rather than the Directory Server Console.

724829 733045	Directory Server Console. Some of these are related to SELinux policies which restrict access to HSMs, and some are due to problems in the Directory Server Console or the Admin Server, which can throw exceptions or fail to generate requests or certificates.	
732079	Upgrading the server fails if the Directory Server user is **root**.	The Directory Server should run as the system user **nobody**.
737144	At least one font must be installed on a system before the Directory Server Console can be launched. Otherwise, the Console fails to open, with a fatal error: `Exception in thread "main" java.lang.Error: Probable fatal error:No fonts found. at sun.font.FontManager.getDefaultPhysicalFont(FontManager.java:1088)` However, because no specific font is required, no font package is listed as a dependency for the Directory Server Console packages.	Install any font package before installing the Directory Server Console packages.
743702	The ***nsslapd-counters*** attribute cannot be set to **off** or the server fails to restart with the error that the counters cannot be found: `[05/Oct/2011:10:07:28 -0400] - slapd stopped. [05/Oct/2011:10:07:42 -0400] - 389-Directory/1.2.9.12 B2011.276.2240 starting up [05/Oct/2011:10:07:42 -0400] - cache_init: slapi counter is not available. [05/Oct/2011:10:07:42 -0400] - ldbm_instance_create: cache_init failed`	The ***nsslapd-counters*** attribute must be set to **on**.

743703	The Directory Server cannot run on the same machine as an NFS share. The Directory Server will stop servicing client requests.	Remove any NFS mount points on the server.

757773	If two Directory Server instances are installed on the same machine and both have SSL enabled, the Directory Server Console cannot be used to managed certificates and can lead to a state where any LDAP operations performed through the Directory Server Console are applied to both instances. The Directory Server Console only accepts the standard SSL port, 636, but the instances must have unique ports. When the Directory Server Console is used for the instance with the non-standard port, it resets the server's port number to 636, and eventually begins applying changes to both instances because the Console connects to both over the same port.	1. Set up the Directory Server to run in SSL, but do not enable SSL for the Directory Server Console yet.
		2. Set the non-standard SSL port in the Directory Server configuration using **`ldapmodify`**. For example:
		`# ldapmodify -x -h server.example.com -p 1389 -D "cn=directory manager" -w secret`
		`dn: cn=config`
		`replace: nsslapd-securePort`
		`nsslapd-securePort: 1636`
		3. Search the Configuration Directory Server for the corresponding SSL port in the administration configuration (**`o=netscaperoot`**). For example:

```
# ldapsearch -x -h
config-
ds.example.com -p
389 -D
"cn=directory
manager" -w secret
-b "cn=slapd-
ID,cn=389
Directory
Server,cn=Server
Group,cn=server.ex
ample.com,ou=exam
ple.com,o=Netscape
Root" -s base
"(objectclass=*)"
nsSecureServerPort

dn: cn=slapd-
ID,cn=389
Directory
Server,cn=Server
Group,cn=server.ex
ample.com,ou=exam
ple.com,o=Netscape
Root
nsSecureServerPort
: 636
```

4. Replace the standard SSL port (636) with the non-standard one. For example:

```
# ldapmodify -x -
h config-
ds.example.com -p
389 -D
"cn=directory
manager" -w secret

dn: cn=slapd-
ID,cn=389
Directory
Server,cn=Server
Group,cn=server.ex
ample.com,ou=exam
ple.com,o=Netscape
Root
replace:
nsSecureServerPort
nsSecureServerPort
: 1636
```

5. Make sure the CA certificate exists in the Admin Server's certificate database and has the

		appropriate trust settings. If the certificate is not in the database, import it and restart the Admin Server. 6. Start the Directory Server Console for the instance. 7. Open the **`Configuration`** tab, and select the top entry in the tree. 8. Open the **`Settings`** tab in the right pane. The **`Encrypted port`** field should show the assigned non-standard port. 9. Open the **`Encryption`** tab, and select the **`Use SSL in Console`** checkbox. 10. Restart the server as prompted.
757836	The **`logconv.pl`** starts its first connection at conn=0 instead of conn=1, but it expects conn=1. This means that the tools misses restarts in the report.	